UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,158	07/25/2003	Adrian Patrick Kent	200206289-1	2520

22879 7590 07/13/2007
HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
POPHAM, JEFFREY D	

ART UNIT	PAPER NUMBER
2137	

MAIL DATE	DELIVERY MODE
07/13/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/627,158	**Applicant(s)** KENT ET AL.	
	Examiner Jeffrey D. Popham	**Art Unit** 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _26 April 2007_.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-49_ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-49_ is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _25 July 2003_ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

Remarks

Claims 1-49 are pending.

Response to Arguments

1. Applicant's arguments with respect to claims 1-49 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-7, 10-13, 16-20, 22-24, 26-38, 41-43, and 46-49 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bennett (Bennett et al., "Experimental Quantum Cryptography", 9/1991, pp. 1-28) in view of Sych (Sych et al., "Quantum cryptography with continuous alphabet", 4/4/2003, pp. 1-14, obtained from http://arxiv.org/PS_cache/quant-ph/pdf/0304/0304035v1.pdf).

Regarding Claim 1,

> Bennett discloses a method of establishing a shared secret random cryptographic key between a sender and a recipient using a quantum communications channel, the method comprising:

Generating a plurality of random quantum states of a quantum entity, each random state being defined by a randomly selected one of a first plurality of bases in Hilbert space (Section 2; note pages 4-5);

Transmitting the plurality of random quantum states of the quantum entity via the quantum channel to the recipient (Section 2; note pages 4-5);

Measuring the quantum state of each of the received quantum states of the quantum entity with respect to a randomly selected one of a second plurality of bases in Hilbert space (Section 2; note pages 4-5);

Transmitting to the recipient composition information describing a subset of the plurality of random quantum states (Section 2; note pages 4-5);

Analyzing the received composition information and the measured quantum states corresponding to the subset to derive a first statistical distribution describing the subset of transmitted quantum states and a second statistical distribution describing the corresponding measured quantum states (Section 2; note pages 4-5);

Establishing the level of confidence in the validity of the plurality of transmitted random quantum states by verifying that the first and second statistical distributions are sufficiently similar (Section 2; note pages 5-6);

Deriving a first binary string and a second binary string correlated to the first binary string, respectively from the transmitted and received plurality of quantum states not in the subset (Section 2; note pages 5-6); and

Carrying out a reconciliation of the second binary string to the first binary string by using error correction techniques to establish the shared secret random cryptographic key from the first and second binary strings (Section 2; note pages 6-7);

But does not disclose the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space and the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space.

Sych, however, discloses the first plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space and the second plurality of bases being randomly and independently chosen from a uniform distribution of all pure quantum states in Hilbert space (Pages 4-8, section III). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the continuous quantum alphabet of Sych into the QKD system of Bennett in order to improve the critical QBER (Quantum Bit Error Rate), allow secure data transmission through practically any noisy quantum channel, and/or allow the system to work at basically any level of external errors or eavesdropping attacks.

Regarding Claim 26,

Claim 26 is a method claim that is broader than method claim 1 and is rejected for the same reasons.

Regarding Claim 35,

Claim 35 is a method claim that is broader than method claim 1 and is rejected for the same reasons.

Regarding Claim 2,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the first and second plurality of bases in Hilbert space each comprise at least four random bases (Section 2, note pages 4-5); and Sych discloses that the first and second plurality of bases in Hilbert space each comprise at least four random bases (Pages 4-8, section III).

Regarding Claim 27,

Claim 27 is a method claim that is broader than method claim 2 and is rejected for the same reasons.

Regarding Claim 36,

Claim 36 is a method claim that is broader than method claim 2 and is rejected for the same reasons.

Regarding Claim 3,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the selecting step comprises generating and measuring a first plurality of bases in two-dimensional Hilbert space (Section 2, note pages 4-5; and Section 3, note page 10); and Sych discloses that the selecting step comprises generating and measuring a first plurality of bases in two-dimensional Hilbert space (Pages 4-8, section III).

Regarding Claim 28,

Claim 28 is a method claim that is broader than method claim 3 and is rejected for the same reasons.

Regarding Claim 4,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the selecting step comprises generating and measuring a first plurality of bases in a real subspace of two-dimensional Hilbert space (Section 2, note pages 4-5).

Regarding Claim 29,

Claim 29 is a method claim that is broader than method claim 4 and is rejected for the same reasons.

Regarding Claim 5,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the composition information transmitting step comprises transmitting information describing the bases of the subset of the plurality of random quantum states (Section 2, note pages 4-5).

Regarding Claim 30,

Claim 30 is a method claim that is broader than method claim 5 and is rejected for the same reasons.

Regarding Claim 6;

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the analyzing step comprises analyzing the information describing the bases to derive the first statistical distribution (Section 2, note pages 4-5).

Regarding Claim 37,

Claim 37 is a method claim that is broader than method claim 6 and is rejected for the same reasons.

Regarding Claim 7,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the establishing step comprises determining a statistical error rate (Section 2, note pages 4-5; and Sections 4-5).

Regarding Claim 38,

Claim 38 is a method claim that is broader than method claim 7 and is rejected for the same reasons.

Regarding Claim 10,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett disclose that the subset information transmitting step comprises transmitting the subset information over a public channel, such as a radio channel (Section 2, note pages 4-5).

Regarding Claim 31,

Claim 31 is a method claim that is broader than method claim 10 and is rejected for the same reasons.

Regarding Claim 11,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the deriving step comprises transmitting information to the recipient representing the bases for the quantum states not in the subset which make up the first binary string (Section 2, note pages 4-5).

Regarding Claim 41,

Claim 41 is a method claim that is broader than method claim 11 and is rejected for the same reasons.

Regarding Claim 12,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that carrying out the reconciliation step comprises using privacy amplification techniques (Section 2, note pages 8-9).

Regarding Claim 42,

Claim 42 is a method claim that is broader than method claim 12 and is rejected for the same reasons.

Regarding Claim 13,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the quantum entity is photons and the quantum states are degrees of polarization of the photons (Section 2, note pages 4-5); and Sych discloses that the quantum entity is photons and the quantum states are degrees of polarization of the photons (Pages 4-8, Section III).

Regarding Claim 32,

Claim 32 is a method claim that is broader than method claim 13 and is rejected for the same reasons.

Regarding Claim 43,

Claim 43 is a method claim that is broader than method claim 13 and is rejected for the same reasons.

Regarding Claim 16,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses determining the second plurality of bases independently of the first plurality of bases (Section 2, note pages 4-5); and Sych discloses determining the second plurality of bases independently of the first plurality of bases (Pages 4-8, Section III).

Regarding Claim 17,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the first and second pluralities of bases are selected randomly (Section 2, note pages 4-5; and Section 3, note page 11); and Sych discloses that the first and second pluralities of bases are selected randomly (Pages 4-8, Section III).

Regarding Claim 18,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses the recipient transmitting some information about the bases chosen for measurement and/or the measurement results to the sender (Section 2, note pages 4-5).

Regarding Claim 47,

Claim 47 is a method claim that is broader than method claim 18 and is rejected for the same reasons.

Regarding Claim 19,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the step of carrying out the reconciliation comprises using several quantum states to generate a single bit of the shared secret at both the sender and recipient (Section 2, note pages 6-9; and Section 5).

Regarding Claim 34,

Claim 34 is a method claim that is broader than method claim 19 and is rejected for the same reasons.

Regarding Claim 48,

Claim 48 is a method claim that is broader than method claim 19 and is rejected for the same reasons.

Regarding Claim 20,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses transmitting data regarding the second statistical distribution from the recipient to the sender (Section 2, note pages 4-5).

Regarding Claim 49,

Claim 49 is a method claim that is broader than method claim 20 and is rejected for the same reasons.

Regarding Claim 22,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that each of the plurality of random quantum states defines two-dimensional information describing the condition of the quantum entity (Section 2, note pages 4-5; and Section 3, note page 10).

Regarding Claim 23,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that each of the plurality of random quantum states define n-dimensional information describing the condition of the quantum entity, where n is three or more (Section 2, note pages 4-5; and Section 3, note page 10).

Regarding Claim 24,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the plurality of random quantum states are arranged geometrically to be uniformly separated within Hilbert space (Section 2, note pages 4-5).

Regarding Claim 33,

Bennett as modified by Sych discloses the method of claim 26, in addition, Bennett discloses that the first plurality of bases is selected randomly (Section 2, note pages 4-5; and Section 3, note page 11); and Sych discloses that the first plurality of bases is selected randomly (Pages 4-8, Section III).

Regarding Claim 46,

Bennett as modified by Sych discloses the method of claim 45, in addition, Bennett discloses that the recipient's plurality of bases is selected randomly (Section 2, note pages 4-5; and Section 3, note page 11); and Sych discloses that the recipient's plurality of bases is selected randomly (Pages 4-8, Section III).

3. Claims 8, 9, 21, 25, 39, and 40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bennett in view of Sych, further in view of Black (Black et al., "Quantum Computing and Communication", 2/20.2002, pp. 1-52).

Regarding Claim 8,

Bennett as modified by Sych discloses the method of claim 1, in addition, Bennett discloses that the establishing step comprises determining a degree of difference between the first and second statistical distributions (Section 2, note pages 6-8; and Pages 20-23); but does not explicitly disclose accepting the security of the channel if a degree of correlation between the two distributions is greater than a threshold level.

Black, however, discloses that the establishing step comprises determining the degree of difference between the first and second statistical distributions; and accepting the security of the channel is the degree of correlation between the two distributions is greater than a threshold level (Pages 35-36). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the error checking technique of Black into the QKD system of Bennett as modified by Sych in order to provide the ability to start over with a completely new key in the event that the error rate is too high, which could indicate a possible interception by an eavesdropper.

Regarding Claim 39,

Claim 39 is a method claim that is broader than method claim 8 and is rejected for the same reasons.

Regarding Claim 9,

Bennett as modified by Sych and Black discloses the method of claim 9, in addition, Black discloses selecting the value of the threshold level (Pages 35-36).

Regarding Claim 40,

Claim 40 is a method claim that is broader than method claim 9 and is rejected for the same reasons.

Regarding Claim 21,

Bennett as modified by Sych does not disclose determining the size of the shared secret to be of the same order as the size of a message to be encrypted with the key.

Black, however, discloses determining the size of the secret shared key to be of the same order as the size of a message to be encrypted with the key (Pages 30-31). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the OTP of Black into the QKD system of Bennett in order to obtain complete security in encryption, such that there is no way to determine a match between the encrypted message and the key.

Regarding Claim 25,

Bennett as modified by Sych discloses a secure communications method for conveying a message from a sender to an intended recipient, the method comprising establishing a shared secret random cryptographic key between a sender and a recipient using a quantum communications channel according to a method as described in claim 1 (see above rejection of claim 1);

But does not disclose using the shared secret key as a one time pad for secure encryption of the elements of the message at the sender; transmitting the encrypted message to the intended recipient using a conventional communications channel; and using the shared secret key as a one time pad for secure decryption of the encrypted elements of the message at the recipient.

Black, however, discloses using the shared secret key as a one time pad for secure encryption of the elements of the message at the sender; transmitting the encrypted message to the intended recipient using a conventional communications channel; and using the shared secret key as a one time pad for secure decryption of the encrypted elements of the message at the recipient (Pages 30-31). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the OTP of Black into the QKD system of Bennett in order to obtain complete security in encryption, such that there is no way to determine a match between the encrypted message and the key.

4. Claims 14, 15, 44, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bennett in view of Sych, further in view of Franson (U.S. Patent 6,678,450).

Regarding Claim 14,

Bennett as modified by Sych does not disclose temporarily storing the received quantum states of the quantum entity prior to carrying out the measuring step.

Franson, however, discloses temporarily storing the received quantum states of the quantum entity prior to carrying out the measuring step (Column 29, line 16 to Column 30, line 31; storage of the quantum entity inherently occurs before the measuring of Bennett as modified by Sych). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the quantum entity storage of Franson into the QKD system of Bennett as modified by Sych in order to allow for caching of information, such that the system can store new quantum information while measuring and processing older quantum information, thereby increasing reliability that data will not be lost.

Regarding Claim 44,

Claim 44 is a method claim that is broader than method claim 14 and is rejected for the same reasons.

Regarding Claim 15,

Bennett as modified by Sych and Franson discloses the method of claim 14, in addition, Franson discloses that the measuring step is carried out after the temporary storing step (Column 29, line 16 to Column 30, line 31); and Bennett discloses using the received recipient composition information to determine some of the bases of the second plurality of bases (Section 2, note pages 4-6).

Regarding Claim 45,

Claim 45 is a method claim that is broader than method claim 15 and is rejected for the same reasons.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D. Popham whose telephone number is (571)-272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2137

Matthew D. Smithers
MATTHEW SMITHERS
PRIMARY EXAMINER
Art Unit 2137